Technical Consultation
for the
Cassini Saturn Orbit Insertion Critical Events Readiness Review

December 2, 2004

Prepared By:
David S. Leckrone, NASA-GSFC

NESC Chief Scientist

Signature Page

NESC Consultation Team

Signatures on file

David S. Leckrone, Chief Scientist

Landis Markley, GSFC

Frank Bauer, NDE – GN&C

Gary Davis, GSFC

EXECUTIVE SUMMARY

After a 10-year journey, the Cassini spacecraft entered orbit around the ringed planet Saturn on July 1, 2004. This critical mission phase, termed Saturn Orbit Insertion (SOI), began with bi-propellant system pressurization on May 20, 2004, and concluded with a final cleanup burn on July 3, 2004. During this time, the Cassini made two crossings of Saturn's ring plane between the F and G rings. In preparation for SOI, the Jet Propulsion Laboratory (JPL) conducted an SOI Critical Events Review (CERR) on April 1, 2004. Mr. Gentry Lee of JPL chaired the CERR. The NESC provided expertise for the CERR and subsequent review activities by assigning Mr. Landis Markley of GSFC, an expert in engineering, development and operations of Guidance, Navigation and Control systems and Mr. Gary Davis, also of GSFC, a propulsion systems expert. An informal report of the findings of the CERR was submitted to the NESC Review Board on April 6, 2004, which constitutes the body of this Position Paper. Major concerns identified that were of particular concern to the NESC reviewers are as follows:

1. Lack of centralized control of entire fault protection system by a single cognizant engineer creates concerns regarding unidentified errors. JPL review of the entire fault protection logic is needed as soon as possible.

2. Operational readiness testing is inadequate, addressing only the spacecraft rather than the entire system. Testing should include simulated contingencies with limited response times, independently observed by outside experts.

3. Failure protection logic automatically switches to the redundant B-side. It is very important that the RCS B-side be tested prior to SOI.

The CERR Board noted the very recent discovery of a design oversight in an operational fault protection system that had been installed after Cassini was launched. This design problem should have been discovered long ago. This raised concerns that other "undiscovered" systems problems might also exist. The Chair of the CERR Board commissioned an in-house study at JPL to search for other "undiscovered" issues. Mr. Landis Markley, representing NESC, participated as an "interested observer" in this follow-up activity, chaired by Ms. Jan Chodas. The final report of this Review Team is attached to this report as Appendix A. The final report of the CERR is attached to this report as Appendix B.

NESC Position Paper

Request Number #: 04-025-E	
Requestor Name: Matt Landano, NCE/JPL	**Requestor Contact Info:** matthew.r.landano@jpl.nasa.gov 818-354-5624
Short Title: Technical Consultation For Cassini Saturn Orbit Insertion (SOI)	
Description: To provide discipline expertise in the areas of Guidance, Navigation and Control (GN&C) systems and propulsion to serve on the Cassini SOI Critical Events Readiness Review (CERR) Board and subsequent related activities.	
Date Received: March 4, 2004	**Date Consultation Initiated:** March 18, 2004
Leads Assigned: David Leckrone, Frank Bauer	**Lead Contact Info:** David.Leckrone@nasa.gov 301-286-5975; Frank.H.Bauer@nasa.gov, 301-286-3102
Date Consultation Concluded: June 18, 2004	

Consultation and Assessment Team

Last Name	First Name	Center	Office Number	Email
Bauer	Frank	GSFC	301-286-3102	Frank.H.Bauer@nasa.gov,
Davis	Gary	GSFC	301-286-3788	Gary.T.Davis@nasa.gov
Landano	Matt	JPL	818-354-5624	matthew.r.landano@jpl.nasa.gov
Leckrone	David	GSFC	301-286-5975	David.Leckrone@nasa.gov
Markley	Landis	GSFC	301-286-4573	Landis.Markley@nasa.gov

CERR Report (prepared by L. Markley)

This is an informal report on the Cassini Saturn Orbit Insertion Critical Events Risk Review (SOI CERR), which was held on April 1, 2004. Mr. Gary Davis (GSFC) and I were the NESC representatives on the review panel, which was chaired by Mr. Gentry Lee of JPL. The chairman did an excellent job of keeping the review focused and allowing ample discussion of important issues while remaining on schedule.

The review was very well presented. The Cassini Project is well prepared for the SOI, with two possible exceptions described below. There has been a significant amount of effort expended to eliminate first-time events at the SOI, by exercising capabilities at the earlier Trajectory Correction Maneuvers TCM-19 (performed in May 2003) and TCM-20 (planned for May 27, 2004). The two problem areas are:

1. The review panel of the Cassini SOI Risk Review, held on October 30, 2003 and also chaired by Mr. Gentry Lee, noted that the Cassini project had taken a piecemeal approach

to the SOI fault protection logic, and recommended that a single engineer be primarily accountable for the entire fault protection development. Cassini Project responded that the complexity of Cassini precluded having a single engineer cognizant of the entire fault protection system. An error in the fault protection logic was uncovered after the Risk Review. This error has been fixed, but the review board is greatly concerned that other errors may also have slipped through the cracks due to the lack of centralized control of the process. Mr. Gentry Lee insisted on an internal JPL review of the entire fault protection logic to be held as soon as possible, probably this week. The SOI CERR panel has been invited to participate if they are available.

2. The proposed Operational Readiness Tests (ORTs) did not appear to be adequate. There should be more tests than were proposed and more complete participation by the entire team involved in the SOI (i.e., Navigation, ECC, and DSN). The current ORTs only address the spacecraft, not the entire system. Several of the tests should include simulated anomalies (“green cards”) unknown to the testers before the tests, emphasizing contingencies with limited response times. There should also be independent observers of the ORTs.

In addition to these major concerns, the review panel raised the following other points:

1. No integrated plan for accomplishing remaining work was presented at the CERR (i.e., how they plan to use people, testbeds, and other facilities between now and SOI.).

2. There should be an earthquake contingency plan. There is a non-negligible possibility that a significant earthquake between now and SOI could take out both JPL and Goldstone.

3. A waiver may be required if the overpressure threshold OP-2 is raised above the qualification level of the propulsion system.

4. More out-of-range testing is required such as AKA break-it testing. The entire range of parameters for both the baseline SOI and out-of-range SOI must be examined.

5. Current plan is to allow a 10-minute cool off period before firing the backup Reaction Engine Assembly (REA) if the primary REA fails. Is this time long enough?

6. Need to write down the logic for employing any redundant hardware.

7. There is still a possibility that the scientists may decide that there is too much debris between Saturn's F and G rings to allow a safe crossing there. They may also recommend moving the crossing of the ring plane to be outside all the rings. It is probably already too late to make this change. No detailed planning of this option has been done since the probability is considered to be too low.

8. Stellar ID is disabled near the rings because of the possibility of misidentifying ring debris as stars. The times of turn-off and turn-on could probably be optimized.

9. The only ground contact with Cassini during the burn is receipt of a beacon signal from the low-gain antennas by the Radio Science Receiver (RSR) through a 70 meter DSN antenna. The Doppler shift of this signal tells how the maneuver is going, so the signal is very important. The center frequencies, bandwidths, and polarizations of the four available RSR channels did not appear to be chosen optimally.

10. No science activities before or during the SOI should be allowed to jeopardize the maneuver.

11. The RCS B-side should be tested before the SOI.

12. Fault protection attitude rate limits at SOI appear to be tighter than necessary.

13. Cassini Project plans to account for any contingencies by modifying the pre-SOI trajectory correction maneuvers TCM-20, TCM-21, and TCM-22 so that the SOI burn is unchanged. Thus, only one specific SOI maneuver is being simulated and rehearsed. Several panel members thought that this was unwise.

Some of these issues will be addressed at internal JPL reviews between now and the SOI.

Appendix A

Cassini SOI Review Team Final Report

Prepared by
Jan Chodas
6/28/04

Background

- Post Cassini launch, AACS and System Fault Protection was added to prevent a failed high pressure latch valve from causing an underburn at SOI.
  - Note that this fault protection was assessed before launch, but deemed unnecessary. The leaky prime regulator and the decision to not switch to the backup regulator drove a change in operations strategy which may not have had adequate review.
- Recently, a design oversight in the added fault protection involving a hardware failure in the latch valve driver was discovered.
- Mr. Gentry Lee (who led an Independent Review Team for SOI) became concerned about the potential for other undiscovered issues and gave Div. 34 an action item to investigate this possibility.

Background (cont'd)

- Jan Chodas coordinated this effort.
  - Review Team Members included Ken Friberg, Mary Lam, Tracy Neilson, Bob Rasmussen, David Skulsky, and Marek Tuszynski.
  - CAS Team Members included Allan Lee, Danny Lam, Larry Chang, Leticia Montanez, Toni Feldman, and Daniel Cervantes.
  - Interested observers included Joe Savino, Landis Markley, Mona Witkowski, and Emily Chen.
- CAS Team Members were overwhelmingly supportive and responsive throughout the effort –

THANK YOU!

Charter

1. Examine how the process broke down and allowed this failure to go undetected for so long.
2. Explore if other process breakdowns are likely to exist.
3. Review the SOI test coverage to check if test holes exist.
4. Identify any Lessons Learned that can be applied to the Probe Relay preparations and to future projects.

Summary of Results

- Examined several aspects of the process.
- Uncovered process weaknesses that call some of the existing FSDS Superscript test case results into question.
- Uncovered weaknesses in the FSDS test environment that implicated the main engine propulsion-related test cases.
- Requested the CAS team run a new set of test cases to spot check design robustness for the SOI burn and reviewed the results. Performed analyses in some key areas.
- Did not uncover any new technical flaw in the SOI design.
- Did not find any unacceptable risks associated with SOI.
- Identified a list of Lessons Learned to apply to the Probe Relay preparations and a list of general Lessons Learned.

Acronyms

- **FSDS -** Flight Software Development System (runs on a Sun workstation). Used to test Attitude Control FSW in non-real-time.
- **FSDS Superscript -** FSDS plus critical SOI sequence (including mark and rollbacks). Used to test Attitude Control FSW FP response interactions with the critical sequence.
- **ITL -** Integration Test Laboratory. Used to test Command Data Subsystem and Attitude Control Subsystem H/W and S/W in real-time.
- **LV -** Latch Valve.

1. Process Breakdown

- **Design:**
  - Reviewed FSC that implemented the LV10 FP coverage.
  - FSC originator doesn't remember why parts of the FSC, which identified changes that might have avoided the design oversight, were not implemented (they show up as strike throughs).
  - Corresponding ECR came before the FSC and matches the FSW implementation.
  - Recent analysis of the FSW change required to protect against this failure found that it would be messy to implement (reason that CAS decided against implementing the change?)

1. Process Breakdown (cont'd)

- **Test:**
  - Regression test for this failed LV driver case was not added to FP regression test suite.
  - Test case with this failure was run as part of FSDS Superscript testing.
  - Test case looked like burn had achieved the desired energy since FSDS does not model the blowdown mode (the expectation was that the latch valve (LV10) would be pyro-bypassed if it failed and thus the burn would be regulated, i.e., no need for blowdown mode).
  - "Pass" criteria used to screen the results didn't catch the fact that LV10 didn't open. Test results were not reviewed manually.
  - Test was not run as part of ITL suite since ITL test cases focused on system/subsystem interactions.

2. Potential for Other Design Breakdowns

- **FSC Review:**
  - Independently reviewed all incorporated A7 and A8 FSCs (385 total).
  - Sent list of questions to CAS Team for those FSCs that were not clear (20 of the 385 FSCs).
  - CAS Team responded to all issues. No similar concerns were uncovered.

2. Potential for Other Test Breakdowns (cont'd)

- **FSDS Model Fidelity:**
  - Propulsion system is not modeled accurately (doesn't model pressures, pressurant latch valve states and pressure system failure modes due to pre-launch assumptions regarding pressure system fault management)
    - Decided that it was not practical to update FSDS with accurate propulsion system model at this late date.
    - Model weakness was not mitigated by ITL test runs since ITL only ran 24 fault injection cases (vs 677 possible faults and 312 fault monitors).
    - Implicates the subset of the 1600 test cases involving the propulsion system.
  - Does not have an accurate mass depletion model (models mass depletion but not inertias).
    - Decided it was not practical to update FSDS with accurate mass depletion model now.
    - Reviewed pertinent analyses and decided that there are no issues.

2. Potential for Other Test Breakdowns (cont'd)

- **FSDS Model Fidelity (cont'd):**
  - FSDS does not support AFC swaps and recovery data (ITL does). Looked into the adequacy of the ITL testing and recommended additional tests. Saw no issues in new tests.
  - FSDS misalignments, biases, etc., may not have latest flight values. Decided that it was too late to vary misalignments and biases for SOI testing, but recommended doing so for Probe Relay testing.
  - FSDS does not have High Water Marks graphical analysis tool to easily determine how much fault margin there is in various test cases. HWM test output data files do exist for all test cases. Developed a tool to post-process HWM data for a subset of cases to assess potential payoff for re-processing data. No issues were found in the 45 old files or the 9 new test cases. Decided to not post-process the remaining files.

2. Potential for Other Test Breakdowns (cont'd)

- "Pass" Criteria:
  - CAS Team explained what the Pass Criteria are and how Pass Criteria were used:
    - A "summary strip" of key information (Delta V achieved, two or more sequence rollbacks, five or more tripped error monitors) was scanned manually for violations.
    - Latch valve states were not displayed.
    - Test results were manually reviewed in only about 10% of the cases.
  - Due to incorrect modeling of latch valve states and consequent blowdown operation, a test case could appear that it achieved desired Delta V, but would not in reality.
  - Looked at the summary strip data types to check if test cases could pass, but in fact not get spacecraft into orbit. Found no issues.
  - Explored whether it was possible to have a sign reversal in commanded burn attitude vectors and not discover it. Found enough checks and balances to preclude erroneous vectors.

2. Potential for Other Test Breakdowns (cont'd)

- FP Monitor Coverage:
  - CAS Team searched through a subset of the FSDS Superscript test case output files and the ITL tests to check if each of the 316 FP monitors (or its companion) tripped at least once.
    - Only used a subset of the Superscript output files that were easily accessible (i.e., not archived).
  - Findings: 137 monitors tripped in FSDS Superscript, 11 in ITL.
  - Reviewed list of untripped monitors and generated a list of 12 monitors to review.
  - CAS Team reviewed the 12 monitors to see if their responses and system interactions are well understood. Found no issues.

2. Potential for Other Test Breakdowns (cont'd)

- **ITL Model Fidelity:**
  - Propulsion model was updated recently and 12 of the 24 SOI fault injection test cases were run with it.
    - Note that this model has limitations due to Ethernet/Sun OS-induced time lags between dynamics model and CDS PMS REU simulation.
    - Reviewed the 12 cases that were not run with the updated model and decided that none needed to be re-run.
  - Mass depletion model is high fidelity.
  - Thruster model has limitations (data dropouts, problems with low rate FSW mode - cannot simulate pulses less than 62.5 ms)
    - Not an issue for SOI, but may be for Probe Relay.
    - Recommended that CAS upgrade the thruster model before running Probe Relay tests since low rate mode may be used.

3. SOI Test Coverage

- **Fault coverage:**
  - A total of 677 faults were injected in FSDS Superscript testing.
  - ITL test cases focused on system/subsystem interactions, not on comprehensive fault injection coverage (only injected 11 AACS faults).
- **Insertion time points:**
  - Faults were injected at up to three discrete time points (all faults were injected once during the burn at a minimum).
- Selected 11 additional test cases to run in either FSDS or ITL by looking at key faults that could prevent the burn from occurring and at many more insertion time points. Analyzed results and observed no show stoppers.
- Analyzed 45 old test cases in detail and did not uncover any show stoppers.

3. SOI Test Coverage (cont'd)

- **Mixed mode (Bus A/Bus B) testing:**
  - ITL did not conduct mixed mode testing. Suggested a test case that starts with some devices on Bus A and some on Bus B, then fails devices in a way that stimulates the "Bus B" idiosyncrasy. Test was run and a FSW behavior idiosyncrasy that can be tolerated was found.
- **Operational workaround for failed latch valve driver:**
  - CAS Team implemented an operational workaround to provide protection for the failed latch valve driver design oversight.
  - Requested an additional 22 test cases be run to try to break the workaround.
  - All test cases performed as expected and validated the workaround.

4. Lessons Learned

- **For Probe Relay Preparations:**
  - Review test case suite for completeness and for appropriateness of the test environment.
  - Confirm that the test environment models reality to the fidelity required for the software to react in a flight-like manner.
  - Run test cases with varying misalignments and biases.
  - Upgrade ITL thruster model for low rate mode (pulses <62.5 ms).
  - Vary fault injection points in time.
  - Save superscript data in a way that makes it easier to post-process.
  - Prototype the data processing approach before executing the test suite.
  - Review all the data or screen it in a way that does not allow failure cases to slip through.
  - Complete the HWM tool to make it easier to use.

Lessons Learned (cont'd)

- **For Future Projects:**
  - Testing is only successful when:
    - The simulation environment is high enough fidelity so that the software will respond in a flight-like manner.
    - The test results are examined objectively and to a level of detail sufficient to catch deviations from a priori expectations.
  - Staff the team with a mix of experienced and new personnel.
  - For long duration developments, emphasize documentation especially during change control process.
  - Augment unit and regression tests as new functionality is added or operations strategy is changed.
  - Review test plans for critical events for completeness.
  - Peer review test strategy and test pass criteria with people with prior experience.
  - Do verification testing by a person independent of the FSW team to ensure that "intent" of function is met.
  - Implement a review process format that digs down to an effective level.
  - Manage resources and priorities throughout development to ensure successful design, implementation and testing.

Conclusions

- SOI test plan relied on ITL tests and on FSDS Superscript tests.
  - Superscript test environment did not model propulsion system state accurately, so test cases involving the propulsion system are suspect.
  - Superscript test case results were not all reviewed in detail.
- Additional test cases that were run to spot check the design and additional analyses that were performed did not uncover any show stoppers.
- Did not find any unacceptable risks associated with SOI.
- Lessons learned for Probe Relay task and for future JPL missions were identified.

Appendix B

April 15, 2004

CASSINI

SATURN ORBIT INSERTION CRITICAL EVENT READINESS REVIEW

prepared by
Gentry Lee

April 1, 2004

Summary Report

The Cassini Critical Event Readiness Review (CERR) for Saturn Orbit Insertion (SOI) was held at the Jet Propulsion Laboratory (JPL) in Pasadena, California, on Thursday April 1, 2004. Mr. Gentry Lee served as Chairman of the review. Review board members in attendance were Bob Barry (JPL), Robert Berry (Lockheed Martin), Dennis Bogan (NASA Headquarters), Frank Carr (Consultant), Mark Dahl (NASA Headquarters), Gary Davis (GSFC/NESC), Jim Gillis (Aerospace), Kevin Johnson (Lockheed Martin), Matt Landano (JPL), Landis Markley (GSFC/NESC), Dennis Matson (JPL), Bob Rasmussen (JPL), and Mark Saunders (NASA-Langley). Attendance from the JPL System Management Office (SMO) included Shyam Bhaskaran, Phil Garrison, Al Nakata, Reid Thomas, and Rod Zieger.

Fundamentally, the purpose of the Cassini SOI CERR was to evaluate the readiness of the Cassini project to accomplish SOI as well as the crucial activities immediately before and after the maneuver. More specifically, the review board was asked to assess (1) if the planned the SOI activities are compliant with the project requirements; (2) if the preparations for these activities are complete; (3) if all the elements of the Cassini project are, or will be, ready to support SOI; (4) if the schedule for the remaining work is achievable; and (5) if the residual risks associated with all the SOI activities are acceptable.

In general, the review board agreed that the Cassini project appears to be well prepared for the SOI activities. Each element of the project crisply identified its tasks throughout the crucial period, and indicated how the preceding work would be accomplished as well as the major risks. The team is strong technically and clearly understands the work to be accomplished. However, several individuals on the review board expressed concerns about possible overconfidence among the Cassini team members. There was one other consensus element of concern among the board members. Top down systems engineering, including schedule and work plan integration, was not highly visible in the review. In fact, there were a few inconsistencies between the navigation team and spacecraft team presentations, indicating that project systems engineering has not yet been completed in a couple of key areas. Because no strong systems engineering presence was demonstrated at the review, a couple of members of the board wondered if the project's obvious confidence is indeed warranted.

An earlier SOI risk review, in October 2003, recommended that the project employ an independent, "properly paranoid", experienced systems engineer to do a penetrating review of the most important phases of the SOI period. This has not yet been accomplished. Based on the CERR, the board feels that it is still of vital importance for the Cassini project to subject itself to intensive independent scrutiny to guard against both overconfidence and complacency.

The major findings and recommendations of the Cassini SOI CERR Review Board are listed below in a more or less prioritized order.

REVIEW BOARD FINDINGS AND RECOMMENDATIONS

1) **Finding:** The project did not demonstrate that it uses, as a regular management tool, a project-wide, integrated work plan and schedule covering all the significant tasks to be completed prior to execution of the SOI phase activities. Although each distributed element of the project seems to understand the remaining work, and asserts that the staffing and time available are both commensurate with the work to be done, it was not possible to verify at the review that all the inter-element tasks have been identified and will be done on a timely basis, or that all the concomitant systems engineering tasks have been properly defined.

Recommendation: Start using an integrated schedule and work plan for the entire project as soon as possible. Status progress against that baseline plan frequently, at least at biweekly intervals. Analyze the plan regularly to determine if any key systems engineering tasks that go across the team elements have been inadvertently omitted.

2) **Finding:** Somewhat surprisingly, considering the test maturity and stability of the SOI sequence and the fault protection design, the Cassini project discovered a major flaw in the AACS fault protection implementation as recently as six weeks prior to the CERR. Although this problem has now been fixed with a software change, and regression testing has been finished, the fact that this significant error was discovered so late raises a red flag about the completeness of the testing process.

Recommendation: Charter immediately an independent review team to investigate in detail the specific AACS fault protection problem that was discovered recently. Have the Cassini project explain to this review team not only why the problem was not identified earlier, but also why the project's responses have precluded the possibility that other similar major software errors have not yet been detected. Extend the purview of this team, as necessary, to include any and all elements associated with the design and testing of the SOI sequence and its fault protection implementation.

3) Finding: The number and scope of planned Operational Readiness Tests (ORTs) for the SOI phase lacks concrete definition and, overall, is inadequate in both breadth and depth. Since the Cassini project does not have a dedicated test and training engineer, and there is a project-wide assumption that the years of cruise experience have basically prepared the Cassini team for any events that might occur during the SOI phase, planning for the ORTs has been proceeding on a somewhat ad hoc basis, leaving the exact details to the individual team elements. As a result, there is considerable fuzziness in how the ORTs will be conducted and how completely they will involve all elements of the MOS/GDS. For example, at the CERR it was disclosed that neither the navigation team nor the DSN is expected to be fully involved in one or more of the critical ORTs.

Recommendation: Hire a dedicated test and training engineer to oversee the ORTs for the SOI phase. Develop a test and training plan, including at least test descriptions, objectives, and pass/fail criteria. Carefully consider the total number of tests, as well as the specific mission phase of each test, taking into account mission criticality, contingency plans, the degree of urgency in required responses, and the experience of the team from all prior activities.

4) Finding: The Cassini design philosophy is to implement a pre-canned SOI maneuver with NO change in ANY state variable. This concept of a fixed SOI is possible because the project intends to use the last pre-Saturn midcourse maneuvers and the post-insertion orbit trim maneuvers to accommodate all statistical variations. The entire previous SOI sequence testing suite has, therefore, basically validated this single, fixed SOI burn. Although the review board agrees with the project that it is unlikely that Cassini will be forced to perform a SOI other than the one tested, there are a few plausible scenarios (such as the occurrence of a significant fault in the reawakened main propulsion system during TCM-20) that could result in the requirement to implement a new and different SOI. At present, the project does not have a disciplined, overall approach to identifying the conditions under which such changes in the baseline SOI would be required, and does not have any plans to do any early “other SOI” testing.

Recommendation: Develop, at the top project level, an overall logic tree defining the branch points leading to the use of a SOI maneuver other than the fixed one that has been recurrently tested. Attempt to define quantitative criteria, including decision times, for activating these contingency branches. When this analysis activity is ongoing, reassess the possible value of pre-testing one or more contingency SOI maneuvers in the test bed.

5) Finding: Major elements of the propulsion system that will be used for SOI have not been exercised for five years. Most of these key elements will be used, purposely, during TCM-

20 prior to the Phoebe encounter, both to characterize the behavior of the overall system and to make certain that everything is ready for SOI. In a sense, TCM-20 is an in-flight test and its results will have a major impact on the implementation of the SOI.

Recommendation: Conduct an official review after the Phoebe encounter as an extended part of the readiness activity. At this review, validate that the performance of TCM-20 does indeed demonstrate propulsion system readiness to implement the fixed, baseline SOI or, alternately, identify at the review any significant untoward results and the impact on SOI and/or SOI preparation activities.

6) Finding: The Cassini project has not yet defined in any detail how it will respond to possible anomalies during TCM-20, such as the failure of a latch valve. There may not be sufficient time after TCM-20 to make such decisions and complete possible checkouts that may be necessary.

Recommendation: Develop logic prior to TCM-20 defining Cassini project response to critical latch valve failures or other system anomalies that influence redundant hardware usage. Include, for each major logic branch, any possible impacts on the SOI implementation sequence.

7) **Finding:** The only real-time data available on Earth during the SOI burn comes from using the low gain antenna as a beacon. This data will provide some information about insertion burn progress and the sequence of events. To acquire this data, a 70 meter DSN station must be available and properly functioning. It is not obvious that the Cassini project has taken unusual steps to try to guarantee that this critical DSN asset is functional during the critical period.

Recommendation: Develop, together with the DSN, a strategy that uses all reasonable methods of guaranteeing the availability of a 70 meter station during the SOI burn.

8) Finding: Although the Cassini project has conducted an independent subsystem evaluation of each of the critical parameters in the onboard software with independent teams from the central divisions, it is not clear that a proper SYSTEMS level independent review of these critical parameters has ever taken place. Historically, subsystem engineers choose fault triggers that are unduly conservative, and often do not properly take into account the mission and system ramifications.

Recommendation: Conduct an independent systems review of a selected set of the most important onboard parameters. Include experienced system and fault protection personnel from other flight projects in the review. Based on the outcome of that review, consider expanding the systems review to encompass a much wider set of onboard parameters.

9) **Finding:** The project has not defined any mission control center contingency plans. There exist plausible scenarios in which an earthquake or some other catastrophe could incapacitate JPL and/or Goldstone.

Recommendation: Evaluate the cost benefit/risk mitigation associated with using Lockheed Martin in Denver, CO as a mission control center during critical SOI activities.

Plan Approval and Document Revision History

Approved:	**Original signature on file** **NESC Director**	**01/04/05** **Date**

Version	Description of Revision	Office of Primary Responsibility	Effective Date